REMARKS

In the Office Action dated April 13, 2006, the Examiner rejected claims 24, 26-30, 32-34 and 36-38 under 35 USC § 102(e) as anticipated by Ho et al. (US 6 850 981) ("Ho"). The Examiner rejected claims 25, 31, 35 and 39-41 under 35 USC § 103 as unpatentable over Ho in view of Aziz et al. (US 6 597 956) ("Aziz").

In this Amendment, Applicant has obviated the § 102(e) rejection. To obviate the rejection, Applicant has cancelled claims 24, 30 and 34 and added the limitations thereof to claims 25, 31 and 35, respectively, and has amended claims 26-29, 32 and 33, and 36-38 to make them dependent on claims 25, 31 and 35, respectively.

Accordingly, the only remaining rejection is the § 103 rejection based on the combination of Ho and Aziz. Applicant traverses that rejection based on the foregoing amendments and the following considerations.

1. THE COMBINATION OF HO AND AZIZ DOES NOT TEACH OR SUGGEST WIRELESS COMMUNICATION WHEREIN A DATA ELEMENT IS SCHEDULED FOR TRANSMISSION PURSUANT TO A TRANSMISSION PRIORITY ENCODED IN AN IEEE 802.1Q TAG OF A REQUEST

All claims as presently amended recite, *inter alia*, wireless communication wherein a data element is scheduled for transmission pursuant to a transmission priority encoded in an IEEE 802.1Q tag of a request to transmit the data element.

In the latest Office Action, the Examiner acknowledges that Ho does not disclose to include an 802.1Q tag in a request or to encode a transmission priority within such an 802.1Q tag. In particular, the Examiner states that "Ho et al. does not disclose that the 802.1Q tag is found within the request." April 13, 2006 Office Action p. 9,

and that "Ho et al. does not disclose that the priority for the data element is encoded in an IEEE 802.1Q tag within the request." Id. at 7-8.

However, the Examiner goes on to note that Aziz mentions using an 802.1Q tag to "control access" and infers from this singular reference that Aziz both describes using an 802.1Q tag in a request and that this use invokes priority information in the 802.1Q tag. In particular, the Examiner states at page 8 of the Office Action:

> Aziz et al., in the field of communications, discloses using an IEEE 802.Q tag within a request (See column 21 lines 31-42 of Aziz et al. for reference to using an 802.1Q tag to control access, meaning the tag is used in the request of access). Using an IEEE 802.Q tag within a request to send data has the advantage of allowing a request to be granted or denied based on information found in the IEEE 802.Q1 tag, which includes data priority information.

Aziz does not disclose what the Examiner claims and the Examiner's reliance on Aziz is misplaced.

Aziz discloses a conventional, security-oriented use of the VLAN ID in an 802.1Q tag to prevent an IP spoofing attack on a network. As stated in Aziz at column 21, lines 18-28:

> According to one embodiment, tight binding between VLAN tagging and IP addresses are used to prevent spoofing attacks by a VSF [Virtual Server Farm] since (physical switch) port-based VLAN tags are not spoofable. An incoming IP packet on a given VLAN interface must have the same VLAN tag and IP address as the logical interface on which the packet arrives. This prevents IP spoofing attacks where a malicious

> server in a VSF spoofs the source IP address of a server in another VSF and potentially modifies the logical structure of another VSF or otherwise subverts the security of computing grid functions.

Stated differently, Aziz recognizes that when controlling access to a network it is inadequate to merely verify that the source IP address in a packet is an authorized IP address because the source of the packet can spoof the source IP address, that is, use a false IP address to gain unauthorized access. Therefore, Aziz instructs to perform a "VLAN/IP address consistency check" (see column 21, line 36) to verify that the source IP address/VLAN ID pair in the packet is an authorized pair before allowing the packet through. Since the VLAN ID is added to the packet at a physical port in the network rather than by the source of the packet, the VLAN ID cannot be spoofed by the source of the packet. Therefore, a packet having a spoofed IP source address will fail to penetrate the network as long as it arrives through a physical port not associated with the rightful owner of the IP address.

As should be now apparent, Aziz's proposed application of an 802.1Q tag to "control access" has no relation whatsoever to requests, priorities, or scheduling transmission. The discussion in Aziz fails to relate what the Examiner claims for at least the following reasons:

a. Aziz at most suggests using an 802.1Q tag to control access of the same packet in which the 802.1Q tag is encoded; it does not suggest using an 802.1Q tag of a request to transmit another packet as recited in the claims.

b. Aziz at most suggests using the VLAN ID portion of an 802.1Q tag; it does not suggest using the priority portion of an 802.1Q tag as recited in the claims.

c. Aziz at most suggests using an 802.1Q tag to determine whether to forward or drop a packet; it does not suggest using an 802.1Q tag to schedule transmission of a packet as recited in the claims.

In summary, the claims as amended are allowable for at least the reason that the prior art of record fails to teach or suggest wireless communication wherein a data element is scheduled for transmission pursuant to a transmission priority encoded in an IEEE 802.1Q tag of a request to transmit the data element.

2. THE COMBINATION OF HO AND AZIZ DOES NOT TEACH OR SUGGEST WIRELESS COMMUNICATION WHEREIN A PARTICULAR DATA ELEMENT IS SCHEDULED FOR TRANSMISSION PURSUANT TO A TRANSMISSION PRIORITY INCLUDED IN A REQUEST TO TRANSMIT THE PARTICULAR DATA ELEMENT

Claims 25-29, 31-33 and 35-38 as amended recite, *inter alia*, wireless communication wherein a particular data element is scheduled for transmission pursuant to a transmission priority included in a request to transmit the particular data element.

In the latest Office Action, the Examiner rejected these claims based on an assertion that the recited "request to transmit a particular data element" finds correspondence in Ho's reservation request for a session/application. Applicant believes the Examiner's position is in error. Ho's session/application reservation request solicits a sustained reservation for transmitting a large number of data elements that belong to a common flow. Ho's session/application reservation request does not address any data element in particular.

By Ho's own admission, its session/application reservation requests reflect a "macro bandwidth management" strategy (see Ho, col. 10, line 20) for reserving link capacity

for transmitting large quantities of data elements that belong to the same flow. The difference between Applicant's request to transmit a particular data element and Ho's session/application reservation requests is manifest in the following definition of "session" from a popular Internet technical dictionary:

> In computer science, in particular networking, a session is either a lasting connection using the session layer of a network protocol or a lasting connection between a user (or user agent) and a peer, typically a server, usually involving the exchange of many packets between the user's computer and the server. A session is typically implemented as a layer in a network protocol (e.g., telnet or FTP).
> Wikipedia, Computer Science Definition of "Session"
> http://www.answers.com/topic/session-computer-science?method=6
> (emphasis added).

This difference between Ho's and Applicant's requests has operational consequences. Ho's "per session" and Applicant's "per data element" reservation styles further substantially different network policies. Ho's requests may be less frequent and therefore require less signaling overhead than Applicant's requests; however, at the same time, Ho's decoupling of bandwidth reservations from the bandwidth requirements of individual data elements may also lead to gross misallocations of bandwidth.

In summary, claims 25-29, 31-33 and 35-38 as amended are allowable for the further reason that the prior art of record fails to teach or suggest wireless communication wherein a particular data element is scheduled for transmission pursuant to a transmission priority included in a request to transmit the particular data element.

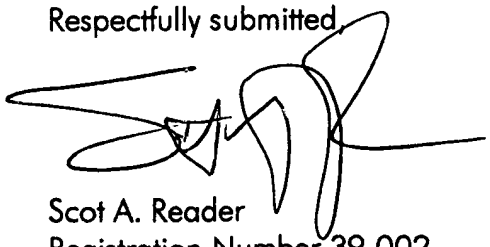
In view of the foregoing, reconsideration and favorable action on all claims are respectfully requested. Accordingly, Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

SUMMARY OF TELEPHONIC INTERVIEW (M.P.E.P. 713.04)

On May 25, 2006, a telephonic interview was conducted at the request of Applicant. Applicant's attorney, Mr. Reader, and the Examiner, Mr. Mattis, participated. The present Amendment and Aziz were discussed. Applicant's attorney stressed that Aziz does not disclose use of an IEEE 802.1Q tag within a request, or use of a priority within an 802.1Q tag, or use of information in an 802.1Q tag to schedule transmission of a packet as recited in the claims as amended. Applicant's amendments of the claims to delete the phrase "within the request" were also discussed briefly. The Examiner stated that in consideration of the present Amendment the Examiner may conduct a further search and that if a rejection were to be issued in the next Office Action, such rejection would not be final.

Should any question remain in view of this communication, the Examiner is encouraged to call the undersigned so that a prompt disposition of this application can be achieved.

Respectfully submitted,



Scot A. Reader
Registration Number 39,002

Telephone No. (303) 440-4050
Scot A. Reader, P.C.
1320 Pearl Street
Suite 228
Boulder, CO 80302